Cassandra Crossing/ Dall'etere ad Ethernet

(325)—Un attacco veicolato attraverso le Smart TV che, tramite una falla nel sistema che gestisce il cambio dei canali, può propagarsi…

Cassandra Crossing/ Dall'etere ad Ethernet

Figure 1:

(325)—Un attacco veicolato attraverso le Smart TV che, tramite una falla nel sistema che gestisce il cambio dei canali, può propagarsi alla rete locale, ai dispositivi connessi, a Internet. Il nemico può nascondersi in salotto e l'industria non se ne cura.

11 luglio 2014—Avremo presto, anzi alcuni di noi hanno già, un nemico in salotto (e forse in camera da letto). E' cosa nota e tecnicamente dimostrata, ma nessuno pare preoccuparsene.

Perché? Dobbiamo fare diversi passi indietro per spiegare, quindi i 24 instancabili lettori dovranno fare uso di tutta la loro pazienza, ma ne varrà la pena.

Scopriremo così che la sicurezza in quanto tale non paga, quindi spesso non ci si cura della sicurezza se non per evitare danni economici.

Leggendo dei problemi di sicurezza che affliggono tutto quanto sia fatto di informatica e telecomunicazioni, ci si pone spesso il problema del perché software, hardware, firmware, telefonia e telecomunicazioni siano mediamente così insicuri. La convinzione più diffusa è che siano errori dei programmatori, problemi di prodotti poco collaudati ed altre questioni legate a particolari e rimediabili problemi.

Chi si occupa più a fondo di almeno uno di questi settori sa che oltre agli "errori" esistono dei problemi intrinseci delle "regole" o protocolli che standardizzano e "governano" appunto gli oggetti informatici e le telecomunicazioni.

Alcuni di questi protocolli, come ad esempio il TCP/IP, sono stati concepiti nei primi anni '70, quando i computer che dovevano scambiarsi i dati erano 7 in tutto. La grande innovazione allora era la commutazione di pacchetto: sicurezza, autenticazione ed autorizzazione non erano nemmeno pensabili. Gli anni sono passati, i computer sono diventati migliaia, poi milioni ed infine miliardi: sono passati da occupare un palazzo intero a stare nelle tasche di tutti.

Le esigenze sono molto cambiate, ma i protocolli sono ancora con noi. E visto che parecchie cose, inclusa la sicurezza, sono diventate indispensabili, è stato necessario creare nuovi protocolli che permettano di usare in maniera sicura quelli vecchi. E' ad esempio il caso dell'SSL che "gira sopra" il vecchio TCP/IP garantendo la sicurezza del vostro conto corrente bancario telematico.

Ma la sicurezza viene presa in considerazione (in misura comunque limitata) solo quando è indispensabile ed è relativamente facile da implementare, come avviene per il software.

Quando invece ad essere coinvolti sono le reti fisiche, ad esempio quelle telefoniche, i cambiamenti sono più lenti e spesso ci si affida alla "*security throught obscurity*", cioè ad una presunta sicurezza ottenuta non tramite progettazioni e protocolli sicuri, ma semplicemente nascondendo, o meglio cercando di nascondere, le informazioni tecniche sui sistemi di telecomunicazioni e sui loro punti deboli.

E' questo che rende, ad esempio, la rete mondiale di telefonia cellulare un sistema dimostratamente non affidabile e facilmente attaccabile. Storie dell'orrore sono davvero accadute, e le parti coinvolte hanno imparato molto.

Esistono consorzi di aziende o di aziende ed enti pubblici che si preoccupano di definire in maniera intelligente e condivisa i nuovi standard, tenendo conto dell'esperienza accumulata su quelli precedenti.Questo entro certi limiti, non in un mondo ideale.

Sempre più frequentemente nel mondo reale gli "standard" servono infatti non per garantire la sicurezza, ma piuttosto per sviluppare o proteggere interessi economici; i sistemi DRM ne sono ottimi esempi.

Anche nella definizione di nuovi standard purtroppo, interessi, errori e desiderio di giustificarli senza correggerli sono sempre in agguato. L'ultimo esempio, "From the Aether to the Ethernet—Attacking the Internet using Broadcast Digital Television" scoperto da un gruppo di ricercatori riguarda la definizione dello standard HbbTV, che definisce le regole di funzionamento delle cosiddette Smart TV, o ricevitori televisivi ibridi.

L'aspetto del protocollo che ci interessa è la distribuzione via onde radio, quindi in broadcast, di contenuti attivi (ma chiamiamoli semplicemente "programmi") destinati ad essere eseguiti sul computer contenuto nella Smart TV ogni volta che si cambia canale.

Questi programmi, che ogni canale TV trasmette indipendentemente se, quando e come vuole, sono utilizzati, usando anche il collegamento ad Internet delle Smart TV, per sovrapporre contenuti interattivi (come siti web) alla trasmissione televisiva. Per inciso, pare siano già avvenuti alcuni casi di impiego illegale di questa caratteristica per eseguire programmi elementari che semplicemente "telefonavano a casa" via internet, per informare "qualcuno" che uno spettatore si era sintonizzato su un certo canale.

Questo tipo di cose è già possibile da anni, grazie all'utilizzo dei ricevitori per digitale terrestre di tipo MHP (quelli del famoso "premi il tasto rosso") che possono essere anche collegati ad un canale di ritorno telefonico o di rete, ma che per fortuna non hanno avuto molta diffusione, anche perché le capacità di calcolo incluse in questi ricevitori sono molto limitate ed i programmi scaricati limitati a codice Java.

Ma il protocollo HbbTV è destinato ad oggetti con potenze di calcolo e connettività ragguardevoli come le Smart TV, la cui diffusione sarà capillare nel giro di pochi anni.

"Solo un problema di sicurezza casalinga in più", penseranno i 24 ingenui lettori.No: non solo il rischio è quantitativamente molto più grave ma deve anche essere considerato su più piani diversi contemporaneamente. Una Smart TV HbbTV ogni volta che cambiamo canale scarica del software leggendolo via radio, e per default lo esegue dopo aver ovviamente controllato che sia fidato.

Sapete come fa a fidarsi? Va a leggere il nome del sito di provenienza e lo confronta con quello di chi gestisce il canale. Sapete da dove arriva il nome? Dal segnale radio stesso.

E' un po' come se un impianto di allarme, per decidere se suonare o no, chiedesse alla persona che sta entrando "Sei il padrone di casa o sei un ladro?" e si fidasse della risposta. Come fare quindi per infettare con un malware una Smart TV?

Basta "clonare" temporaneamente una trasmittente TV legittima usando hardware radio standard e software liberamente disponibile (una Software Defined radio come GNUradio è un ottimo punto di partenza), registrare uno spezzone del canale che si vuole compromettere, iniettarvi le opportune informazioni di identificazione, aggiungervi come carico pagante il malware prescelto, inviarlo ad una trasmittente DVB via USB ed infine ad un amplificatore a radiofrequenza amatoriale dotato di una bella antenna a stilo omnidirezionale.

Il segnale così trasmesso sovrasterà per intensità quello legittimo in un raggio da 100 a 500 metri, ogni Smart TV in quel raggio (che tanto "smart" non è…) lo elaborerà, visualizzerà lo stream audio, riprodurrà lo stream video, e dopo aver controllato se il nome di chi gestisce il canale torna, eseguirà il codice in arrivo sul canale dati.

Pochi secondi di interferenza sono sufficienti: se il raggio di infezione non bastasse, un po' di "Smartdriving" ne amplificherà molto l'effetto.Il fatto di essere arrivato via radio rende l'attacco assolutamente non tracciabile a posteriori: niente IP, niente MAC, niente tabulati.

Il fatto di durare pochi secondi lo rende irrintracciabile (perché non triangolabile) anche dal punto di vista radio.Un fantasma che infetta le SmartTV, insomma. Cosa può fare il software proveniente dall'etere? Più o meno tutto, ma la cosa più originale sarebbe se infettasse la vostra rete locale e tutti i vostri gadget… dall'interno, propagandosi poi anche via Internet per buon peso.

Chi vorrà leggersi la pubblicazione (davvero interessante) potrà infine bearsi del finale estremamente educativo.

Dopo aver scoperto il problema del protocollo, molto responsabilmente gli autori non l'hanno divulgato ma sottoposto all'attenzione dell'associazione che gestisce il protocollo HbbTV.

La risposta è stata che non era un problema reale, e che nulla sarebbe stato modificato, perché il profilo economico dei possibili attacchi li rendeva non appetibili. Sulla sicurezza dei futuri utenti, nessuna considerazione.

Così gli autori, oltre a pubblicare tutto, hanno anche stimato il valore economico di una serie di possibili attacchi in relazione al costo dell'apparecchiatura, e l'hanno incluso nella pubblicazione.Non c'è minimamente da stupirsi.

Questa è la sicurezza tipica dell'elettronica di consumo.

Originally published at punto-informatico.it.